UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/759,182	01/20/2004	John Brawner Duffie III	10-008	7709

23164 7590 09/04/2007

LEON R TURKEVICH
2000 M STREET NW
7TH FLOOR
WASHINGTON, DC 200363307

EXAMINER	
SERRAO, RANODHI N	
ART UNIT	**PAPER NUMBER**
2141	

MAIL DATE	DELIVERY MODE
09/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/759,182	DUFFIE ET AL.	
	Examiner	Art Unit	
	Ranodhi Serrao	2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 July 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22,27-31,34-37 and 39-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22, 27-31, 34-37, and 39-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments, see remarks, filed 13 July 2007, with respect to the rejection(s) of claim(s) 1-22, 27-31, 34-37, and 39-42 under 35 U.S.C. have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of newly found prior art reference(s).

2. The applicant argued in substance the limitations of independent claims 1, 10, 18, and 27, dependent claim 40, and the newly added claims 41 and 42. However, the newly cited prior art references teach these and the added features. See below rejections.

Claim Rejections - 35 USC § 103

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 1, 10, 18, 27, and 40-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maeshima et al. (6,092,113) and MeLampy et al. (2003/0051130).

5. As per claim 1, Maeshima et al. teaches a method in a router having at least one outbound interface (see Maeshima et al., col. 4, line 66-col. 5, line 2), the method comprising: establishing, on the outbound interface, a plurality of Internet Protocol (IP)-based secure connections with respective destinations based on receiving encrypted packets generated by a cryptographic module (see Maeshima et al., col. 4, lines 1-18);

controlling supply of data packets to the cryptographic module by: (1) assigning, for each secure connection, a corresponding queuing module, and outputting to the cryptographic module the group of data packets, from each corresponding queuing module according to the corresponding assigned output bandwidth, for generation of the encrypted packets (see Maeshima et al., col. 5, lines 45-64) and second outputting the encrypted packets from the cryptographic module to the one outbound interface for transport via their associated secure connections (see Maeshima et al., col. 6, lines 10-27). But fails to teach each encrypted packet successively output from the cryptographic module having a corresponding successively-unique sequence number; (2) reordering, in each queuing module, a corresponding group of the data packets associated with the corresponding secure connection according to a determined quality of service policy and based on a corresponding assigned maximum output bandwidth for the corresponding queuing module. However, MeLampy et al. teaches each encrypted packet successively output from the cryptographic module having a corresponding successively-unique sequence number (see MeLampy et al., ¶ 15); (2) reordering, in a queuing module, a corresponding group of the data packets associated with the secure connection according to a determined quality of service policy and based on a assigned maximum output bandwidth for the queuing module (see MeLampy et al., ¶ 29-35). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify Maeshima et al. to each encrypted packet successively output from the cryptographic module having a corresponding successively-unique sequence number; (2) reordering, in each queuing module, a corresponding group of the data

packets associated with the corresponding secure connection according to a determined quality of service policy and based on a corresponding assigned maximum output bandwidth for the corresponding queuing module in order to prevent any person from eavesdropping on the communication by providing encryption for rerouting multi-media data flow packets (see MeLampy et al., ¶ 11-13).

6. Claims 18 and 27 have similar limitations as to claim 1; therefore, they are being rejected under the same rationale.

7. As per claim 10, Maeshima et al. teaches a router comprising: an outbound interface configured for establishing a plurality of Internet Protocol (IP)-based secure connections with respective destinations based on receiving respective streams of the encrypted packets (see Maeshima et al., col. 4, lines 1-18); a queue controller configured for controlling supply of data packets to the cryptographic module, the queue controller configured for assigning, for each secure connection, a corresponding queuing module, each queuing module configured for: (1) outputting to the cryptographic module a corresponding group of the data packets with the corresponding secure connection, and according to a corresponding assigned output bandwidth for the corresponding queuing module for generation of the corresponding stream of the encrypted packets (see Maeshima et al., col. 5, lines 45-64). But fails to teach a cryptographic module configured for successively outputting encrypted packets having respective successively-unique sequence numbers; and (2) reordering the corresponding group of the data packets according to a determined quality of service policy and the corresponding assigned maximum output bandwidth. However,

MeLampy et al. teaches a cryptographic module configured for successively outputting encrypted packets having respective successively-unique sequence numbers (see MeLampy et al., ¶ 55); and (2) reordering the corresponding group of the data packets according to a determined quality of service policy and the assigned maximum output bandwidth (see MeLampy et al., ¶ 29-36). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify Maeshima et al. to a cryptographic module configured for successively outputting encrypted packets having respective successively-unique sequence numbers; and (2) reordering the corresponding group of the data packets according to a determined quality of service policy and the corresponding assigned maximum output bandwidth in order to prevent any person from eavesdropping on the communication by providing encryption for rerouting multi-media data flow packets (see MeLampy et al., ¶ 11-13).

8. As per claim 40, Maeshima-MeLampy teach a method, wherein: the router includes the outbound interface, the cryptographic module, and each of the queuing modules; the establishing of the IP-based secure connections, the controlling supply of data packets, and the second outputting of the encrypted packets to the outbound interface each executed in the router (see Maeshima et al., col. 5, lines 3-42).

9. As per claim 41, Maeshima-MeLampy teach a method, further comprising: selecting one of the outbound interfaces for each of the data packets by a routing circuit in the router based on receiving the data packets from at least one inbound interface in the router; the second outputting including outputting each encrypted packet to the

corresponding selected one of the outbound interfaces selected by the routing circuit (see Maeshima et al., col. 6, lines 7-27).

10. As per claim 42, Maeshima-MeLampy teach a router, further comprising a routing circuit configured for selecting one of a plurality of the outbound interfaces for each said data packet, the cryptographic module configured for outputting each encrypted packet to the corresponding selected one of the outbound interfaces selected by the routing circuit (see Maeshima et al., col. 6, lines 7-27).

11. Claims 2-9, 11-13, 16, 17, 19-22, 25-26, 28-31, 34, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maeshima et al. and MeLampy et al. as applied to claim 1 above, and further in view of Young et al. (2003/0093563).

12. As per claim 2, Maeshima et al. and MeLampy et al. teach the mentioned limitations of claim 1 above but fail to teach a method, wherein the reordering step includes, in each queuing module, reordering the corresponding group of the data packets according to the determined quality of service policy in response to detection of a congestion condition in the outbound interface. However, Young et al. teaches a method, wherein the reordering step includes, in each queuing module, reordering the corresponding group of the data packets according to the determined quality of service policy in response to detection of a congestion condition in the outbound interface (see Young et al., ¶ 9). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify Maeshima et al. and MeLampy et al. to a method, wherein the reordering step includes, in each queuing module, reordering the

corresponding group of the data packets according to the determined quality of service policy in response to detection of a congestion condition in the outbound interface in order to implement a complete customer premise solution that enables secure, reliable and manageable delivery of voice, video and data services over common IP connections (see Young et al., ¶ 2).

13. Claims 11, 19, and 28 have similar limitations as to claim 2; therefore, they are being rejected under the same rationale.

14. As per claims 3-9, the above-mentioned motivation of claim 2 applies fully in order to combine Maeshima et al., MeLampy et al., and Young et al.

15. As per claim 3, Maeshima et al., MeLampy et al., and Young et al. teach a method, wherein the reordering step includes, in each queuing module: establishing a plurality of queues having respective identified priorities (see Young et al., paragraph 0051); storing each data packet associated with the corresponding secure connection in one of the queues based on a corresponding identified priority for said each data packet (see Young et al., paragraph 0019); and selectively outputting the stored data packets from the queues, according to the corresponding quality of service policy (see Young et al., paragraph 0009).

16. Claims 12, 20, and 29 have similar limitations as to claim 3; therefore, they are being rejected under the same rationale.

17. As per claim 4, Maeshima et al., MeLampy et al., and Young et al. teach a method, wherein: the establishing step includes establishing, on each of a plurality of the outbound interfaces (see Young et al., paragraph 0080), a corresponding plurality of

the secure corrections with a corresponding plurality of respective destinations based on receiving a corresponding stream of encrypted packets from the cryptographic module (see Young et al., paragraph 0082); the controlling step includes controlling the supply of data packets, for each outbound interface, from the cryptographic module based on repeating the assigning, reordering, and outputting steps for each of the secure connections (see Young et al., paragraph 0150); the second outputting step including outputting each encrypted packet to a corresponding one of the outbound interfaces according to a routing decision executed by the router (see Young et al., paragraph 0098).

18. Claims 21 and 30 have similar limitations as to claim 4; therefore, they are being rejected under the same rationale.

19. As per claim 5, Maeshima et al., MeLampy et al., and Young et al. teach a method, wherein the second outputting step includes outputting the encrypted packets for transport via their associated secure connections according to IP Security (IPSEC) protocol (see Young et al., paragraph 0123).

20. Claims 13, 22, and 31 have similar limitations as to claim 5; therefore, they are being rejected under the same rationale.

21. As per claim 6, Maeshima et al., MeLampy et al., and Young et al. teach a method, wherein the determined quality of service policy implements a guaranteed quality of service for one of a video stream and an audio stream (see Young et al., paragraph 0053).

22. Claim 14 has similar limitations as to claim 6; therefore, it is being rejected under the same rationale.

23. As per claim 7, Maeshima et al., MeLampy et al., and Young et al. teach a method, wherein the audio stream is a Voice over IP media stream (see Young et al., paragraph 0053).

24. Claim 15 has similar limitations as to claim 7; therefore, it is being rejected under the same rationale.

25. As per claim 8, Maeshima et al., MeLampy et al., and Young et al. teach a method, wherein the controlling step further includes obtaining, for each queuing module, the corresponding assigned maximum output bandwidth from a configuration register (see Young et al., paragraph 0051).

26. Claims 16, 25, and 34 have similar limitations as to claim 8; therefore, they are being rejected under the same rationale.

27. As per claim 9, Maeshima et al., MeLampy et al., and Young et al. teach a method, wherein the controlling step further includes negotiating, for at least one queuing module, the corresponding assigned maximum output bandwidth with the corresponding destination (see Young et al., paragraphs 0085-0087).

28. Claims 17, 26, and 35 have similar limitations as to claim 9; therefore, they are being rejected under the same rationale.

29. Claim 36-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maeshima et al. and MeLampy et al. as applied to claim 1 above, and further in view of Haney (7,111,163).

30. As per claim 36, Maeshima et al. and MeLampy et al. teach the mentioned limitations of claim 1 above but fail to teach a method, wherein each secure connection is a corresponding encrypted tunnel. However, Haney teaches a method, wherein each secure connection is a corresponding encrypted tunnel (see Haney, col. 8, lines 10-44). It would have been obvious to one having ordinary skill in the art at the time of the invention to modify Maeshima et al. and MeLampy et al. to a method, wherein each secure connection is a corresponding encrypted tunnel in order to solve the quality of service problem by providing non-blocking bandwidth (bandwidth that will always be available and will always be sufficient) and predefining routes for the "private tunnel" paths between points on the internet between ISX facilities (see Haney, col. 4, line 62-col. 5, line 6).

31. Claims 37-39 have similar limitations as to claim 36; therefore, they are being rejected under the same rationale.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ranodhi Serrao whose telephone number is (571) 272-7967. The examiner can normally be reached on 8:00-4:30pm, M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on (571) 272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

RNS
R.N.S.

8/31/2007

WILLIAM VAUGHN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100